



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/696,200

10/28/2003

David M. Chess

GB920030050US1

7325

66517

7590

12/14/2007

STEVEN E. BACH, ATTORNEY AT LAW

10 ROBERTS ROAD

NEWTOWN SQUARE, PA 19073

EXAMINER

HOANG, DANIEL L

ART UNIT

PAPER NUMBER

2136

MAIL DATE

DELIVERY MODE

12/14/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

AK

<b>Office Action Summary</b>	<b>Application No.</b> 10/696,200	<b>Applicant(s)</b> CHESS ET AL.	
	<b>Examiner</b> Daniel L. Hoang	<b>Art Unit</b> 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 11 July 2007.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-14 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-14 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### DETAILED ACTION

In view of the Appeal Brief filed on 7/10/07, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-14 are rejected under 35 U.S.C. 102(b) as being anticipated by Jordan US

PGP No. 20020073323.

**As per claim 1, 8 and 14 Jordan teaches:**

A method for detecting malicious software within or attacking a computer system, said method comprising the steps of:

*[see paragraph 18]*

in response to a system call, executing a hook routine at a location of said system call to

(a) determine a data flow or process requested by said call,

*[see paragraph 20, "... process of recognizing attempts to restricted system resources.."]*

(b) determine another data flow or process for data related to that of said call,

*[see paragraph 20, "monitoring both the emulation of the computer executable code and the computer system memory state"]*

(c) automatically generate a consolidated information flow diagram showing said data flow or process of said call and said other data flow or process, and after steps (a-c),

*[see paragraph 27, " While the program file is being emulated, monitor component 32 monitors the code execution and any modifications of memory state (step 12), and supplies to detector component 33 information regarding the emulated code execution and any modifications of memory state by the emulated code execution. Based on the information supplied by monitor component 32, detector component 33 detects an attempt by the emulated code to access one or more of the restricted computer system resources (step 13)"]*

*[it is hereby noted that paragraph 0009 of applicant's specification cites that information flow diagrams are known for use in analyzing software during development.]*

(d) call a routine to perform said data flow or process requested by said call.

*[see paragraph 20, "...emulating computer executable code.."]*

#### **As per claim 2, Jordan teaches:**

A method as set forth in claim 1, wherein a user monitors said information flow diagram and compares the data flow or process of steps (a) and (b) with a data flow or process expected by said user.

*[see paragraph 27, " While the program file is being emulated, monitor component 32 monitors the code execution and any modifications of memory state (step 12), and supplies to detector component 33 information regarding the emulated code execution and any modifications of memory state by the emulated code execution. Based on the information supplied by monitor component 32, detector component 33 detects an attempt by the emulated code to access one or more of the restricted computer system resources (step 13)"]*

#### **As per claim 3 and 9, Jordan teaches:**

A method as set forth in claim 1, wherein said information flow diagram illustrates locations of said data at stages of a processing activity.

Art Unit: 2136

*[see paragraph 0027, "Examples of operations monitored include the installation of a new exception handler followed by forcing of a corresponding exception and/or the installation of a new interrupt handler followed by forcing of a corresponding interrupt."]*

**As per claim 4 and 10, Jordan teaches:**

A method as set forth in claim 1, wherein said system call is selected from the set of: open file, copy file to memory, copy memory to register, mathematical functions, write to file, and network or communication functions.

*[see paragraph 0024, "A similar viral technique may be applied to interrupt handlers. Interrupts are used by other devices in a system to gain attention of the processor. For example, when an input/output device (for example, printer, modem, etc.) is ready to send/receive data to/from the processor, the device notifies the processor via an interrupt. An interrupt handler is a specified computer code routine in the operating system which handles a corresponding interrupt, when the interrupt is issued by a device in the system."]*

**As per claim 5 and 11, Jordan teaches:**

A method as set forth in claim 1, wherein said system call is a software interrupt of an operating system.

*[see rejection of claim 4]*

**As per claim 6 and 12, Jordan teaches:**

A method as set forth in claim 1, wherein said system call causes a processor to stop its current activity and execute said hook routine.

*[see rejection of claim 1 wherein execution of computer executable code is emulated in order to verify the existence of malicious code.]*

**As per claim 7 and 13, Jordan teaches:**

A method as set forth in claim 1 wherein said system call is made by malicious software.

*[see paragraph 27]*

---

### CONCLUSION

- \* Any response to this Office Action should be **faxed to (571) 273-8300 or mailed to:**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**Hand-delivered responses** should be brought to

Customer Service Window  
Randolph Building  
401 Dulaney Street  
Alexandria, VA 22314

- \* Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

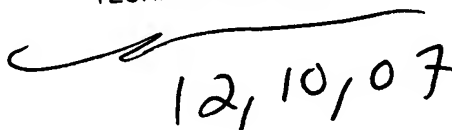
*Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).*



Daniel L. Hoang

12/10/07

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100



12, 10, 07